OO 홈페이지

모의해킹 2팀

모의해킹 결과 보고서

2020.11.02

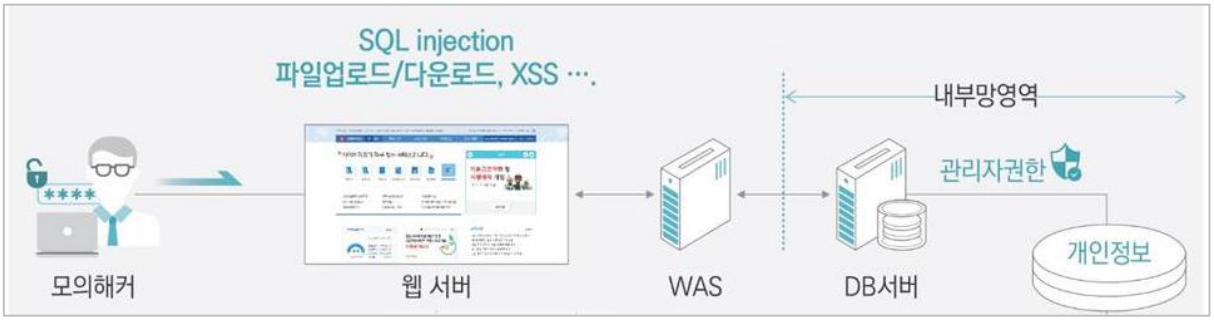
목 차

1. 수행개요

1.1 배경 및 목적

본 취약점 진단은 OO의 웹사이트에 대해 "주요 정보통신 기반시설 기술적 진단 가이드" 진단 항목을 기준으로 존재하는 취약점을 발견하고 취약점을 증명함으로써 해킹 위협으로부터 안전성 여부를 판단함과 동시에 보안 대응책을 강구함을 목적으로 한다.

1.2 수행 범위



[그림 1] 수행 서버 구성도

사이트명	주소
OO 웹 사이트	OO

[표 1] 수행 범위

1.3 수행 전략

1.3.1 정보 수집

- OSINT를 활용한 웹 정보를 수집한다.

  * SHODAN : https://www.shodan.io/

  * Censys : https://censys.io/

- 정보 수집 도구를 활용하여 웹 정보를 수집한다.

수집 도구	사용 목적
whatweb	서버의 구성요소 및 사용된 기술 식별
Nmap	네트워크 스캐닝
Wireshark	네트워크 패킷 분석

[표 2] 활용한 정보 수집 도구

1.3.2 취약점 진단

- 주요정보통신기반시설 취약점 가이드를 기반으로 웹 취약점 진단을 수행한다.

- 취약점 진단을 통해 확인된 취약점을 목록화한다.

1.3.3 모의 침투

- 파악된 취약점 목록을 활용하여 시나리오를 수립한다.

- 수립한 시나리오를 기반으로 한 모의 침투를 진행한다.

1.4 수행 일정

<2020.10.26(월) ~ 2020.11.04(수)>

수행일정	26(월)	27(화)	28(수)	29(목)	30(금)	2(월)	3(화)	4(수)
수행계획서 작성								
정보 수집								
취약점 진단								
모의 침투								
결과 보고서 작성								
프로젝트 발표								

[표 3] 수행 계획

1.5 수행 인원

팀	성명	비고
모의해킹 2팀	정형수	팀장
	김재원	
	이호웅	
	김상훈	

[표 4] 수행 인원

1.6 수행 내용

1.6.1 수행 기준

	항목 중요도	항목코드
버퍼 오버플로우	상	BO
포맷스트링	상	FS
LDAP 인젝션	상	LI
운영체제 명령 실행	상	OC
SQL 인젝션	상	SI
SSI 인젝션	상	SS
XPath 인젝션	상	XI
디렉터리 인덱싱	상	DI
정보 누출	상	IL
악성 콘텐츠	상	CS
크로스사이트 스크립팅	상	XS
약한 문자열 강도	상	BF
불충분한 인증	상	IA
취약한 패스워드 복구	상	PR
CSRF	상	CF
세션 예측	상	SE
불충분한 인가	상	IN
불충분한 세션 만료	상	SC
세션 고정	상	SF
자동화 공격	상	AU
프로세스 검증 누락	상	PV

파일 업로드	**상**	FU
파일 다운로드	**상**	FD
관리자 페이지 노출	**상**	AE

[표 5] 취약점 점검 리스트

1.6.2 수행 내용 상세

- 대표 홈페이지 대상 취약점 진단 실시 / 개발기 내 웹 사이트 대상 진단한다.

- 취약점에 따른 침투 시나리오 작성 및 구현한다.

- 시나리오 기반 모의해킹 및 결과분석한다.

- 취약점 별 영향도 분석 / 시나리오별 위험도 분석 평가 실시한다.

- 침투 결과에 따른 웹 서비스 안전성 확보 방향 제시한다.

1.7 기대효과

- 홈페이지 모의해킹을 통한 데이터 유출 가능성 사전탐지 및 예방한다.

- 주요정보통신기반시설 취약점 가이드를 포함하는 웹 해킹 취약점 해소를 통한 안전성 확보한다.

- 개인정보 유출 등의 해킹 사고 발생시 법적 책임 완화한다.

- 홈페이지 취약점 발견을 통해 위험도 측정을 통한 대응방안 제시한다.

- 고객에게 안정적 서비스를 제공하여 기업 이미지 향상한다.

2. 모의해킹 진단결과

2.1 웹 모의해킹 취약점 항목

OO 홈페이지 취약점 진단을 수행한 결과 **SQL 인젝션, 디렉토리 인덱싱, 정보누출, 크로스 사이트 스크립팅, 불충분한 인증, 불충분한 인가, 불충분한 세션 만료, 세션 고정, 자동화 공격, 프로세스 검증 누락, 파일 업로드, 파일 다운로드, 관리자 페이지 노출, 데이터 평문 전송, 쿠키 변조**까지 총 15개 항목에서 취약점이 도출되었다.

구분	시스템	취약점 항목	비고
1	(구) KISEC 홈페이지	SQL 인젝션	
		디렉토리 인덱싱	
		정보 누출	
		크로스 사이트 스크립팅	
		불충분한 인증	
		불충분한 인가	
		불충분한 세션 만료	
		세션 고정	
		자동화 공격	
		프로세스 검증 누락	
		파일 업로드	
		파일 다운로드	
		관리자 페이지 노출	
		데이터 평문 전송	
		쿠키 변조	

[표 6] 취약점 항목

2.2 웹 모의해킹 취약점 권고사항

SQL 인젝션, 디렉토리 인덱싱, 정보 누출, 크로스 사이트 스크립팅, 불충분한 인증, 불충분한 인가, 불충분한 세션 만료, 세션 고정, 자동화 공격, 프로세스 검증 누락, 파일 업로드, 파일 다운로드, 관리자 페이지 노출, 데이터 평문 전송, 쿠키 변조 총 15개 항목의 취약점에 대한 권고사항은 아래와 같다.

구분	취약점 항목	코드	권고 사항
1	SQL 인젝션	SI	각 게시판의 검색기능에 SQL 인젝션 취약점이 존재한다. 위 취약점을 이용 시 웹에서 데이터베이스의 정보 및 내용을 탈취 가능하다. 아이디, 패스워드, 이름 등 개인정보 탈취, 동일 계정을 이용하는 타 사이트를 이용하여 사용자들에게 2차 피해 발생 가능성이 있다. 인젝션이 발생 가능한 문자의 필터링을 구현하여, 필터링 기능을 강화해야 한다.
2	디렉토리 인덱싱	DI	OO 페이지에 디렉토리 인덱싱 취약점이 존재한다. 공격자는 해당 취약점이 존재하면 브라우저를 통해 특정 디렉토리 내 파일 리스트를 노출하여 응용시스템의 구조를 외부에 허용할 수 있고, 민감한 정보가 포함된 설정 파일 등이 노출될 경우 보안상 심각한 위험을 초래할 수 있어서 웹 서버 설정을 변경하여 디렉토리 파일 리스트가 노출되지 않도록 설정해야 한다.
3	정보 누출	IL	로그인 시 반환되는 response 값 헤더에 서버의 버전 정보가 들어있다. 서버 정보 노출로 취약한 버전 사용이 취약점이 노출될 수 있어서 서버 정보 노출 설정을 변경 해야 한다.
4	크로스 사이트 스크립팅	XS	1대1문의, 회원탈퇴, 검색창, 수강 신청 내 문의사항에서 XSS공격 구문 삽입이 가능하다. 웹 애플리케이션에서 사용자 입력 인수 값에 대한 필터링이 이루어지지 않을 경우, 사용자 인수 값을 받는 웹 사이트 게시판, URL 등에 악의적인 스크립트(자바스크립트, VB 스크립트, ActiveX, 플래

			시 등)를 삽입하여 게시글이나 이메일을 읽는 사용자의 쿠키(세션)를 도용하거나 악성코드(URL 리다이렉트)를 유포할 수 있어서 웹 사이트의 게시판, 자료실, URL 등에서 사용자로부터 입력받는 인수 값에 대해 검증 로직을 추가하거나 인수 값이 입력되더라도 실행되지 않게 하고, 부득이하게 게시판에서 HTML을 사용하는 경우 HTML 코드 중 필요한 코드에 대해서만 입력할 수 있도록 설정해야 한다.
5	불충분한 인증	IA	회원정보수정 페이지에 접근할 때 불충분한 인증 취약점이 존재한다. 중요 정보(회원정보 등) 페이지에 대한 인증 절차가 불충분할 경우 발생하는 취약점으로 권한이 없는 사용자가 중요 정보 페이지에 접근하여 정보를 유출하거나 변조할 수 있으므로 중요 정보 페이지에는 추가적인 인증 철자를 구현해야 해서 중요 정보 페이지에 대한 추가 인증 로직 추가 구현이 필요하다.
6	불충분한 인가	IN	웹 페이지의 1대1문의 내용을 idx값을 변경함으로써 다른 사람의 1대1문의 내용을 확인, 수정할 수 있는 불충분한 인가 취약점이 존재한다. 공격자는 중요 정보 페이지 접근을 위한 인증 로직이 구현되지 않아 1대1문의 같은 페이지에 접근 및 중요 정보의 열람 및 변조를 할 수 있기 때문에 중요 정보 페이지의 추가 인증 로직 구현이 필요하다.
7	불충분한 세션 만료	SC	세션의 만료 기간을 정하지 않거나, 만료일자를 너무 길게 설정하여 공격자가 만료되지 않은 세션 활용이 가능하다.
8	세션 고정	SF	사용자가 로그인할 때 세션 ID가 고정되어 다른 사용자가 로그인된 세션 ID 값을 대입하여 접속 가능한 취약점이 존재한다. 사용자 로그인 시 항상 일정하게 고정된 세션 ID가 발행되는 경우 세션 ID를 도용한 비인가자의 접근 및 권한 우회가 가능하여서 사용자가 로그인할 때마다 예측 불가능한 새로운 세션 ID 생성 로직 구

			현하고 기존 세션 ID는 파기해야 한다.
9	자동화 공격	AU	OO 페이지에서 접근 시도 횟수 제한을 설정하지 않고 자동화 공격을 방치하면, 웹사이트를 다운시키거나 무차별 대입 공격으로 인해 사용자 계정을 탈취할 수 있고, 데이터 등록 또는 메일 발송 기능 등을 이용하여 악의적인 활용이 가능하다.
10	프로세스 검증 누락	PV	mypage의 URL을 입력하여 접근하였을 때 미흡한 인증으로 정상적으로 접근할 수 있다. 비 로그인 시 접근버튼만 비활성화 할 것이 아니라 페이지 자체적으로 세션 확인을 하여 접근을 제한해야 한다.
11	파일 업로드	FU	웹 페이지의 공지사항에 파일 업로드 시 공격자가 조작한 Server Side Script 파일을 업로드 할 수 있는 취약점이 존재한다. 공격자는 해당 취약점을 이용하여 조작된 Server Side Script 파일을 업로드 하고 실행하여, 쉘 권한 획득 후 웹 브라우저를 통해 시스템 관리자 권한 획득 또는 인접 서버에 대한 침입을 시도할 수 있어서 업로드 되는 파일에 대한 확장자 검증 및 실행 권한을 제거해야 한다.
12	파일 다운로드	FD	웹 페이지의 f-NGS Lab페이지에 있는 테스트 파일입니다. 라는 게시물에 파일 다운로드 취약점이 존재한다. 공격자는 해당 취약점을 이용하여 웹 사이트의 파일 다운로드 관련 애플리케이션의 인수 값을 조작하여 웹 사이트의 중요한 파일(DB 커넥션 파일, 애플리케이션 파일 등)이나 웹 사이트를 운용 중인 웹 서버 루트에 있는 중요한 설정 파일을 다운로드할 수 있다. 또한 웹 사이트상에서 파일을 다운받게 해주는 CGI, JSP, PHP, PHP 3 등의 애플리케이션에서 입력되는 인수 값의 유효성을 검증하지 않는 경우 임의의 문자(../ .. 등)나 주요 파일명의 입력을 통해 웹 서버의 홈 디렉터리를 벗어나서 임의의 위치에 있는 파일을 열람하거나 다운받는 것이 가능하므로 다운로드 시 정해진 경로 이외의 디렉터리와 파일에 접근할 수 없도록 구현해

			야 한다.
13	관리자 페이지 노출	AE	OO 페이지에 관리자 페이지 노출 취약점이 존재한다. 공격자는 유추하기 쉬운 URL로 인해 관리자 페이지 및 메뉴 접근이 가능하고 웹 관리자의 권한이 노출될 경우 홈페이지의 변조뿐만 아니라 취약성 정도에 따라서 웹 서버의 권한까지도 노출될 수 있어서 유추하기 어려운 이름(포트 번호 변경 포함)으로 관리자 페이지를 변경하여 쉽게 추측하여 관리자 페이지에 접근할 수 없도록 하고 근본적인 해결을 위해 지정된 IP만 관리자 페이지에 접근할 수 있도록 제한하여야 한다.
14	데이터 평문 전송	SN	페이지 통신이 암호화되지 않고 평문으로 전송되고 있다. 민감한 데이터가 전송되는 구간은 HTTPS 통신을 적용하여 통신 암호화 조치가 필요하다.
15	쿠키 변조	CC	OO 페이지의 쿠키 값 변조로 admin권한 접속이 가능하며 정상적으로 admin 권한을 사용할 수 있는 취약점이 존재한다. 쿠키는 클라이언트에 전달되는 값으로 중요 정보로 구성되므로 이 정보의 조작을 통해 다른 사용자의 유효한 세션을 취득할 수 있으며, 기타 중요 정보의 유출 및 변조가 발생할 위험이 존재하기 때문에 쿠키 대신 Server Side Session 방식을 사용하거나, 쿠키를 통해 인증 등 중요한 기능을 구현해야 할 경우엔 안전한 알고리즘(SEED, 3DES, AES 등)을 적용해야 한다.

[표 7] 취약점 권고사항

3. 상세 진단결과

3.1 SQL 인젝션

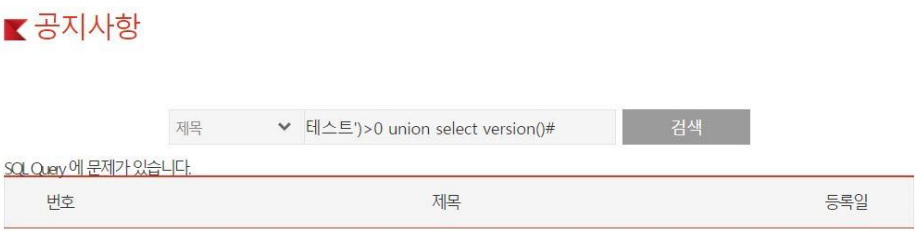
취약점 항목	내용
취약점 설명	웹 파라미터에 SQL 구문을 이용하여 쿼리를 조작할 수 있는 취약점으로, DB 내의 개인정보가 유출되어 2 차공격의 중요한 정보를 제공할 수 있는 취약점이다.
점검 결과	SQL 인젝션 발생할 수 있는 취약한 파라미터를 확인하였다.
위험요소	DB의 정보 유출, 사용자 개인정보 유출 가능성이 존재한다.
발생 경로	OO
보안 대책	SQL 구문을 입력하지 못하도록 필터링을 강화한다.

[표 8] SQLi 취약점 개요

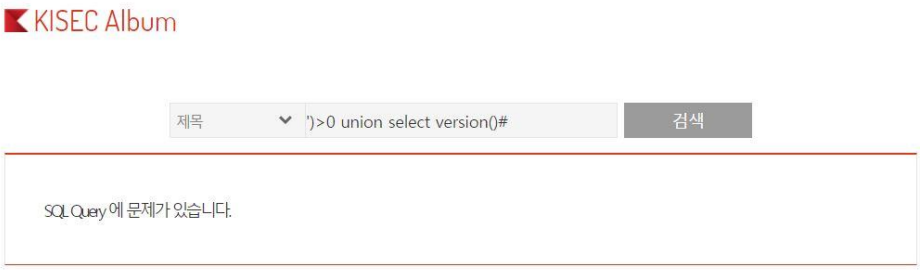
❏ **수행 과정**

SQLi 에러 구문이 출력된다.

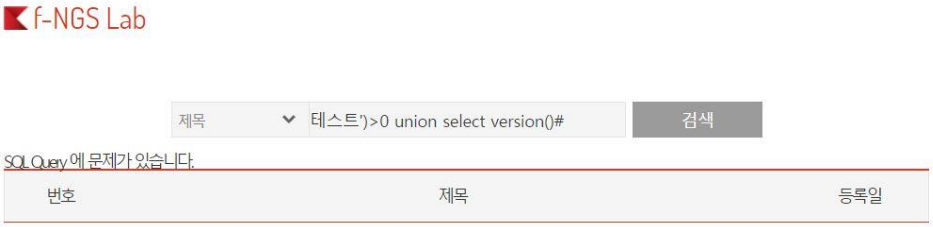
[그림 2] 로그인 SQLi



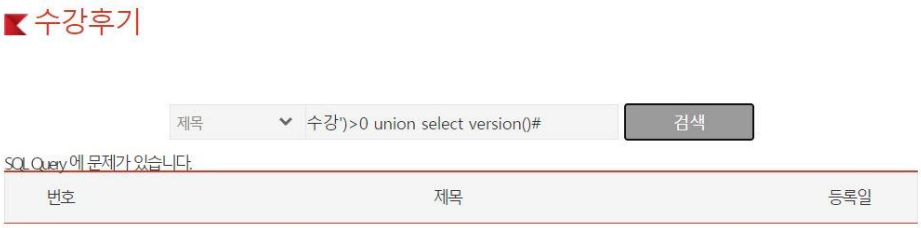
[그림 3] 공지사항 검색 SQLi



[그림 4] Album 검색 SQLi



[그림 5] f-NGS Lab 검색 SQLi



[그림 6] 수강후기 검색 SQLi

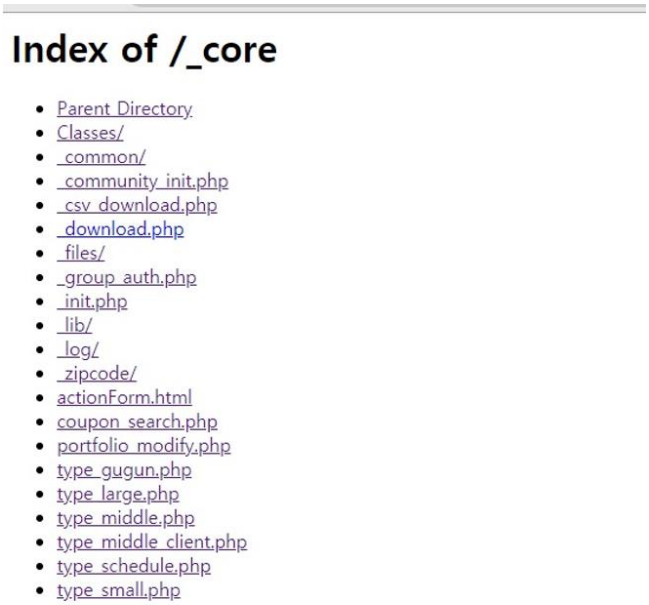
3.2 디렉토리 인덱싱

취약점 항목	내용
취약점 설명	요청 파일이 존재하지 않을 때 자동적으로 디렉토리 리스트를 출력하는 취약점으로 외부에 노출되지 않은 파일까지 노출이 될 수 있는 취약점이다.
점검 결과	외부에 노출되어 있지 않은 파일을 얻을 수 있다.
위험요소	내부의 중요파일 및 경로 유출 가능성이 존재한다.
발생 경로	OO
보안 대책	웹 서버의 설정을 수정하여 indexes을 비활성화 조치해야 한다.

[표 9] 디렉토리 인덱싱 취약점 개요

❏ **수행 과정**

외부로 노출되어 있지 않은 파일을 얻을 수 있다.



[그림 7] 외부에 공개되지 않은 파일

3.3 정보 누출

취약점 항목	내용
취약점 설명	웹 사이트의 민감한 정보(소스코드 내 계정 및 비밀번호, 애플리케이션정보, DB정보, 웹서버 구성 정보, 개발 과정의 코멘트 등)가 노출되어 공격자들의 2차 공격을 위한 정보로 활용될 수 있다.
점검 결과	PHP 이스터에그 페이지를 통해 PHP 버전을 추측할 수 있다. 로그인 성공 시 반환되는 헤더 값에 서버 정보가 노출된다.
위험요소	PHP 버전이 5.5버전 아래의 버전인 것을 알 수 있다. 로그인 성공 시 반환되는 헤더 값으로 버전을 알 수 있다.
발생 경로	OO
보안 대책	PHP설정 파일인 php.ini에 expose_php=OFF 설정을 추가하여 해결 가능하다. Aapache 설정파일의 ServerTokens 값을 Prob로 변경한다.

[표 10] 정보 누출 취약점 개요

❑ 수행 과정

사이트 URL에 이스터에그 구문 입력시 정보 노출이 된다.

PHP Credits

PHP Group
Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski, Jim Winstead, Andrei Zmievski

Language Design & Concept
Andi Gutmans, Rasmus Lerdorf, Zeev Suraski, Marcus Boerger

PHP Authors	
Contribution	**Authors**
Zend Scripting Language Engine	Andi Gutmans, Zeev Suraski, Stanislav Malyshev, Marcus Boerger, Dmitry Stogov
Extension Module API	Andi Gutmans, Zeev Suraski, Andrei Zmievski
UNIX Build and Modularization	Stig Bakken, Sascha Schumann, Jani Taskinen
Windows Port	Shane Caraveo, Zeev Suraski, Wez Furlong, Pierre-Alain Joye
Server API (SAPI) Abstraction Layer	Andi Gutmans, Shane Caraveo, Zeev Suraski
Streams Abstraction Layer	Wez Furlong, Sara Golemon
PHP Data Objects Layer	Wez Furlong, Marcus Boerger, Sterling Hughes, George Schlossnagle, Ilia Alshanetsky

[그림 8] PHP 이스터에그

```
1 HTTP/1.1 200 OK
2 Date: Mon, 02 Nov 2020 10:49:50 GMT
3 Server: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.2g PHP/5.3.25
4 X-Powered-By: PHP/5.3.25
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Content-Length: 99
9 Connection: close
10 Content-Type: text/html; charset=utf-8
```

[그림 9] 반환되는 헤더의 정보 노출

3.4 크로스 사이트 스크립팅

취약점 항목	내용
취약점 설명	악의적인 사용자가 공격하려는 사이트에 스크립트를 실행시켜 사용자의 민감한 정보를 탈취 가능하다.
점검 결과	1대1 문의 사이트, 공지사항 검색 창에 악성 스크립트를 실행 가능하다.
위험요소	사용자의 민감정보를 탈취 가능하다.
발생 경로	OO
보안 대책	사용자로부터 입력받은 인수 값에 대해 검증 로직을 추가하거나 인수 값이 입력되더라도 실행되지 않게 문자열 특수 기호등을 변환 함수를 사용하여 치환하여 저장한다.

[표 11] 크로스 사이트 스크립팅 취약점 개요

❑ 수행 과정

공지사항 검색 창에 크로스 사이트 스크립트구문을 입력한다.

[그림 10] 공지사항 검색 창 스크립트 구문 입력

[그림 11] 스크립트 구문 실행

1대1 문의내용 입력창에 스크립트 구문 실행 가능하다.

문의날짜	2020-10-30 18:45:02
문의분류	분류선택
문의제목	test
문의내용	<script>alert(document.cookie);</script>

[그림 12] 스크립트 구문 작성

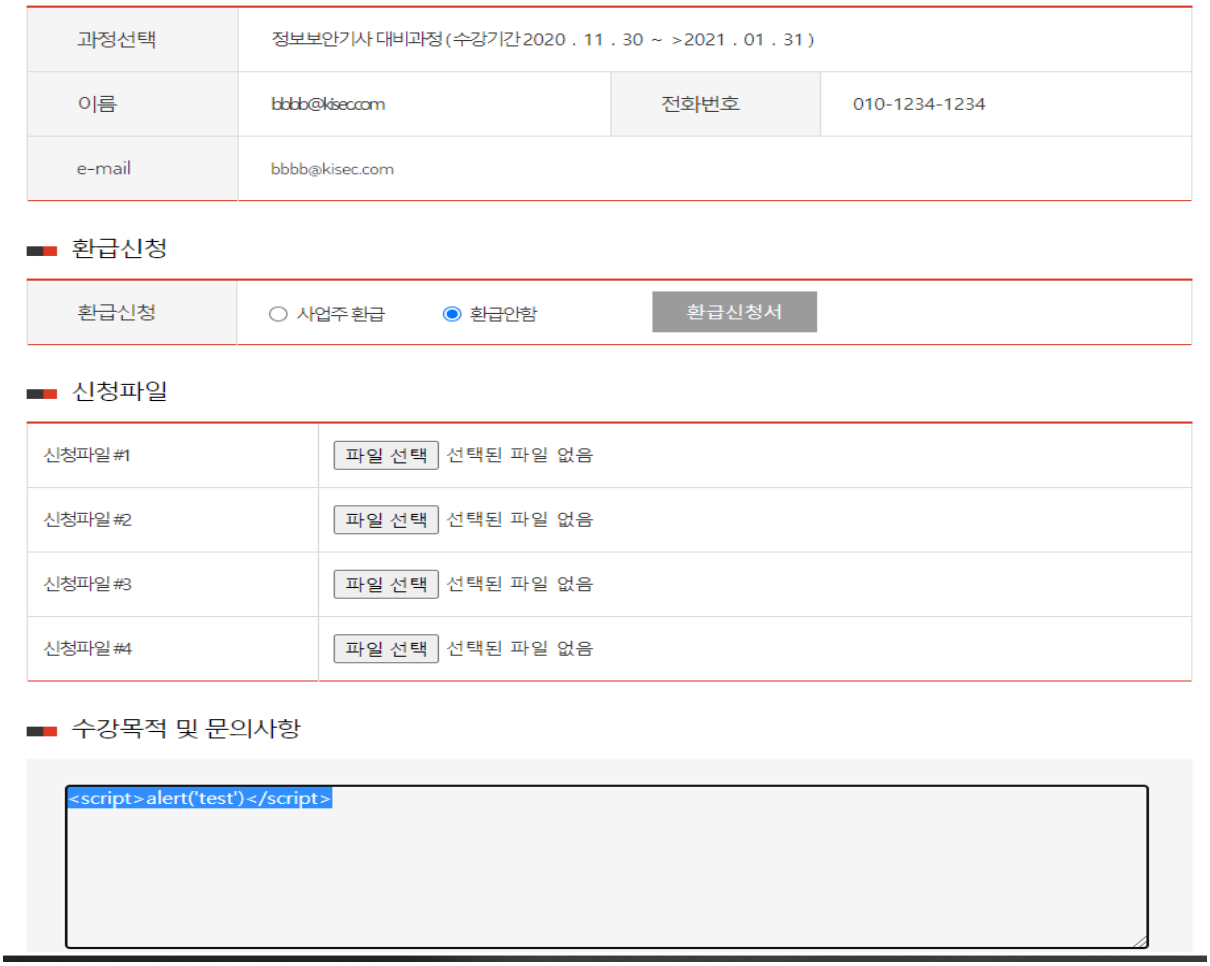
[그림 13] 스크립트 구문 실행

회원탈퇴 사이트에서 탈퇴내용 스크립트구문 내용 전송가능하다.

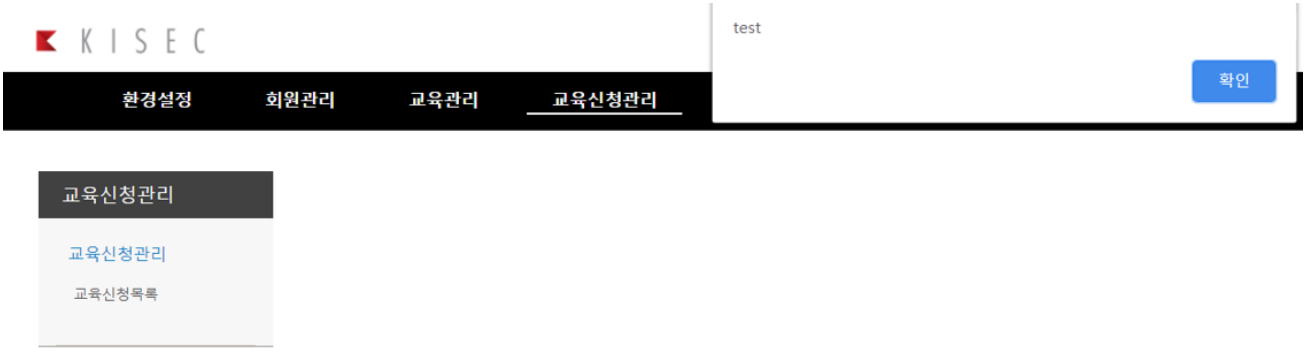
[그림 14] 스크립트 구문 작성

[그림 15] 스크립트 구문 실행

수강신청 문의내용 스크립트 구문 실행가능하다.



[그림 16] 스크립트 구문 작성



[그림 17] 스크립트 구문 실행

관리자페이지에서 게시판항목에서 FAQ에 답변 입력 창에 스크립트 구문 실행 가능하다.

[그림 18] 스크립트 구문 작성

[그림 19] 스크립트 구문 실행

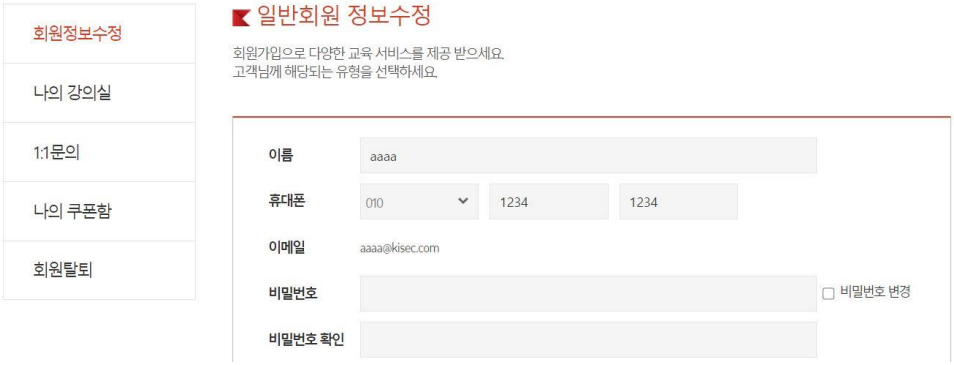
3.5 불충분한 인증

취약점 항목	내용
취약점 설명	중요 정보(회원정보 등) 페이지에 대한 인증 절차가 불충분한 경우 발생하는 취약점으로 권한이 없는 사용자가 중요 정보 페이지에 접근하여 정보를 유출하거나 변조할 수 있다.
점검 결과	2차 인증이 구현되어 있지 않아 로그인만 하면 탈퇴, 정보수정이 가능하다. 회원가입시 비밀번호 강도 확인을 클라이언트에서 진행하고 서버에서 인증 재검증 하지 않는다.
위험요소	세션, 계정 정보 등이 탈취되면 비밀번호를 몰라도 탈퇴, 정보변경이 가능하다. 회원가입 시 취약한 패스워드로 회원가입이 가능하다.
발생 경로	OO
보안 대책	중요페이지에 대한 추가 인증 로직 구현 및 서버에서 재인증 로직 구현해야 한다.

[표 12] 불충분한 인증 취약점 개요

❑ 수행 과정

추가 인증 로직 없이 중요페이지에 접근 가능하다.



[그림 20] 회원정보수정 추가 인증 로직 불충분

[그림 21] 회원탈퇴 추가 인증 로직 불충분

```
function checkPassword(password){

  if(!/^(?=.*[a-zA-Z])(?=.*[!@#$%^*+=-])(?=.*[0-9]).{8,12}$/.test(password)){

    alert('숫자+영문자+특수문자 조합으로 8자리 이상 사용해야 합니다.');
    return false;
  }

  var checkNumber = password.search(/[0-9]/g);
  var checkEnglish = password.search(/[a-z]/ig);
  if(checkNumber <0 || checkEnglish <0){
    alert("숫자와 영문자를 혼용하여야 합니다.");
    return false;
  }
  if(/(Ww)WlWlWl/.test(password)){
    alert('같은 문자를 4번 이상 사용하실 수 없습니다.');
    return false;
  }

  return true;
}
```

[그림 22] 클라이언트에서 패스워드 강도 확인

[그림 23] 취약한 패스워드(1234)로 가입 성공

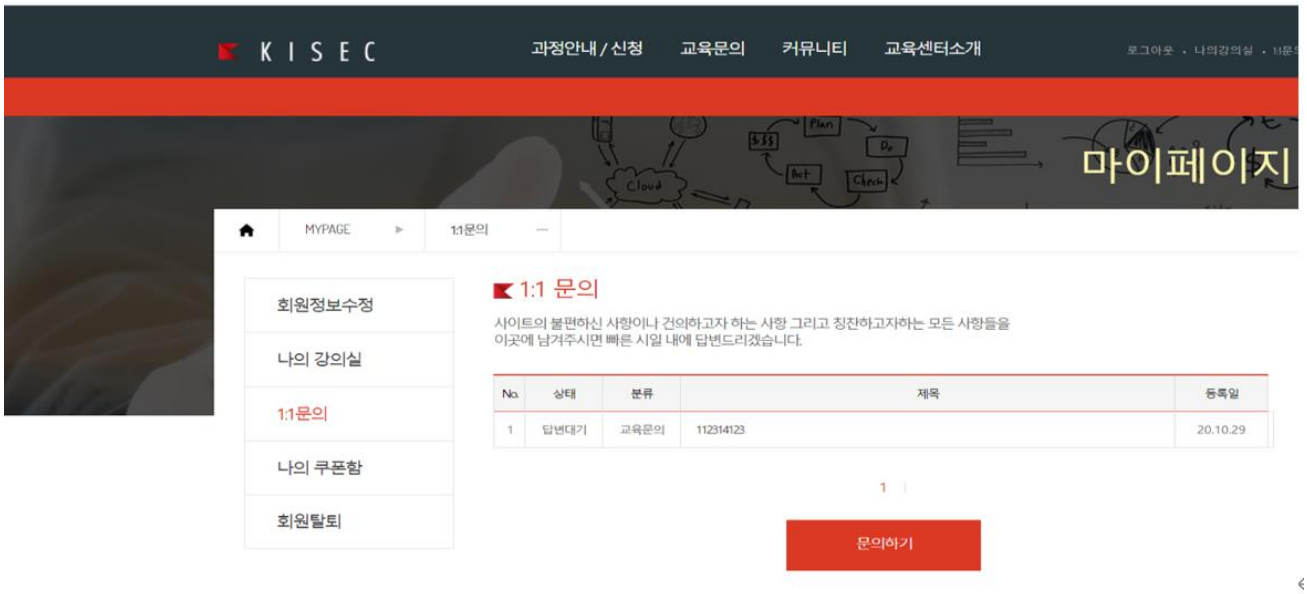
3.6 불충분한 인가

취약점 항목	내용
취약점 설명	중요 정보 페이지 접근을 위한 인증 로직이 구현되지 않을 경우, 비인가 사용자의 페이지에 접근 및 중요 정보의 열람 빛 변조가 가능하다.
점검 결과	다른사람이 작성 게시글 확인 및 수정이 가능하다.
위험요소	권한이 없는 게시글의 수정, 확인이 가능하다.
발생 경로	OO
보안 대책	중요 정보 페이지의 추가 인증 로직 구현해야 한다.

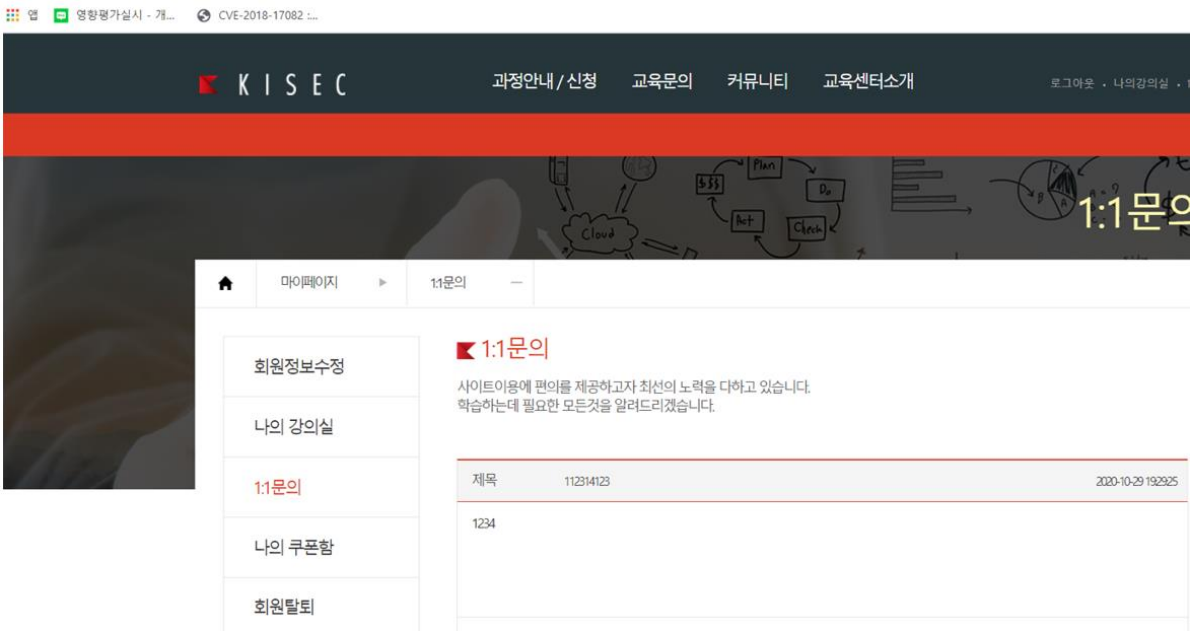
[표 13] 불충분한 인가 취약점 개요

❏ **수행 과정**

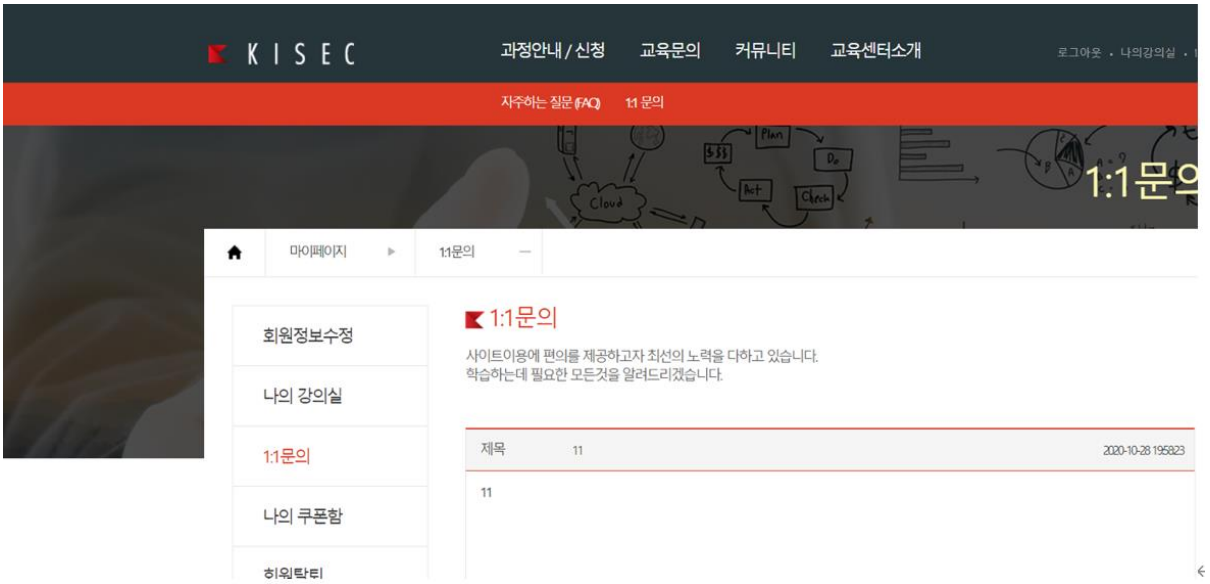
1:1 게시판에서 다른사람의 게시글 보기 가능하다.



[그림 24] 1대1 문의 게시글 화면

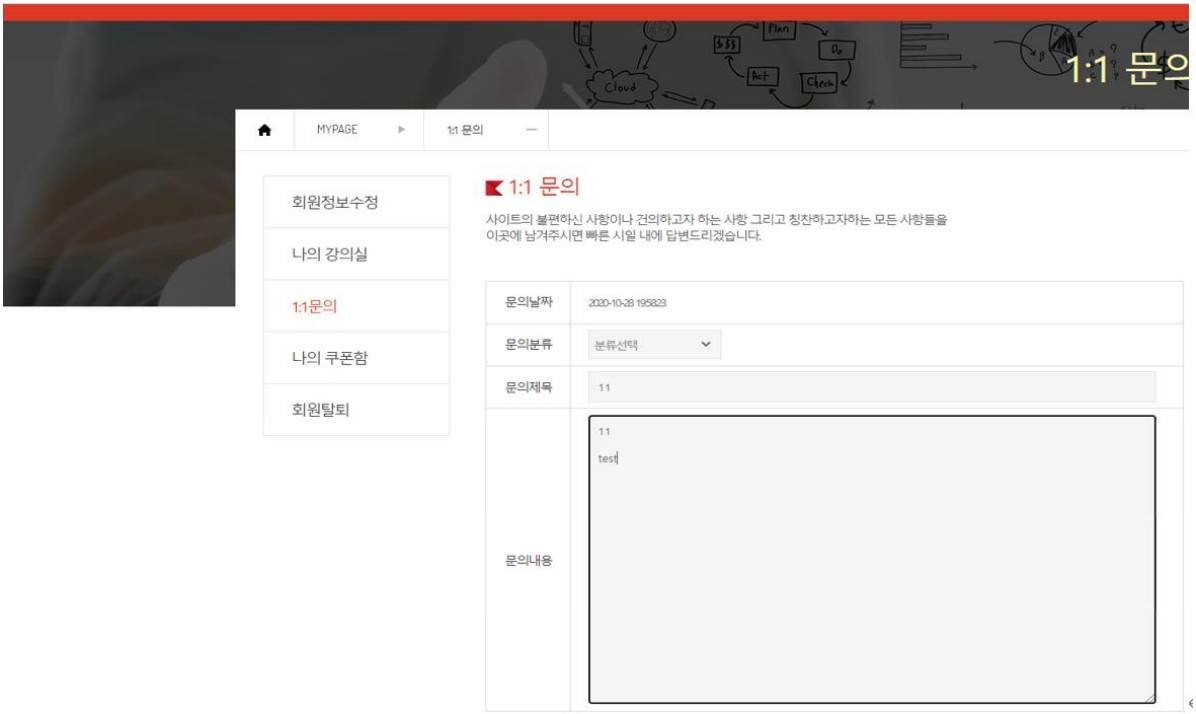


[그림 25] 1대1 문의 게시글 로그인한 유저 글 화면

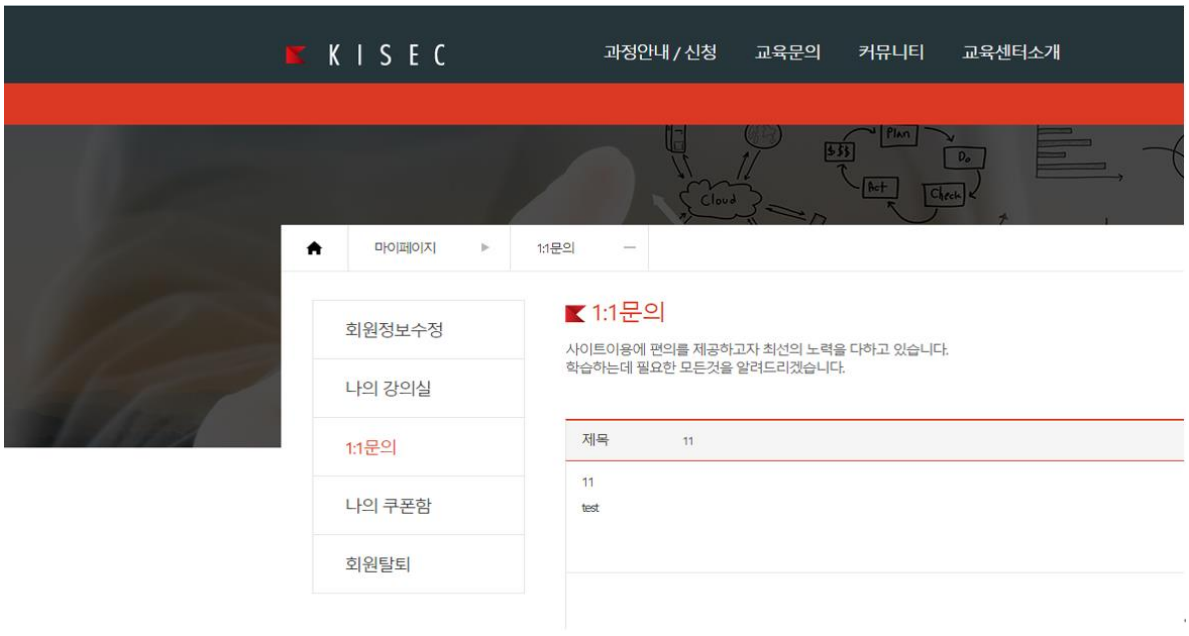


[그림 26] 1대1 문의 게시글에서 타 유저글 화면

1:1게시판에서 다른사람의 게시글 수정 가능하다.



[그림 27] 1대1 문의 게시글에서 타 유저글 수정화면



[그림 28] 1대1 문의 게시글에서 타 유저글 화면

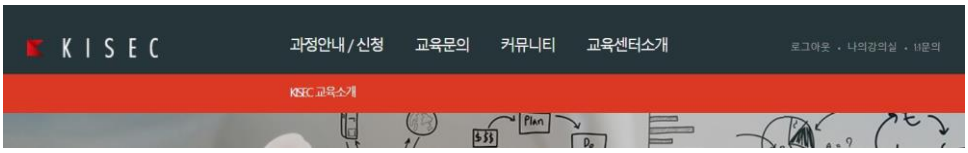
3.7 불충분한 세션 만료

취약점 항목	내용
취약점 설명	세션의 만료 기간을 정하지 않거나, 만료일자를 너무 길게 설정하여 공격자가 만료되지 않은 세션 활용이 가능하게 되는 취약점이다.
점검 결과	10분이 지나도 세션이 만료되지 않는다.
위험요소	세션의 재활용이 가능하다.
발생 경로	OO
보안 대책	세션 만료 설정 및 Timeout 지정해야 한다.

[표 14] 불충분한 세션만료 취약점 개요

❏ **수행 과정**

10분이 지나도 세션이 만료되지 않는다.



[그림 29] 새로고침 후 세션이 만료되지 않음

3.8 세션 고정

취약점 항목	내용
취약점 설명	세션값을 고정하여 명확한 세션 식별자(ID) 값으로 사용자가 로그인하여 정의된 세션 식별자(ID)가 사용 가능하게 되는 취약점이다.
점검 결과	사용자 로그인 시 항상 일정하게 고정된 세션ID가 발행한다.
위험요소	사용자 로그인 시 항상 일정하게 고정된 세션ID가 발행되는 경우 세션 ID를 도용한 비인가자의 접근 및 권한 우회가 가능하다.
발생 경로	OO
보안 대책	로그인 할 때마다 예측 불가능한 새로운 세션 ID가 발행되고, 기존 세션 ID는 파기해야 한다.

[표 15] 세션 고정 취약점 개요

❏ **수행 과정**

세션값이 계속 유지된 사용하는 상태이다.

[그림 30] 로그인한 유저 세션 값 확인

[그림 31] 로그인한 유저 세션 값 변경

[그림 32] 로그인한 유저 과거 세션값 입력화면

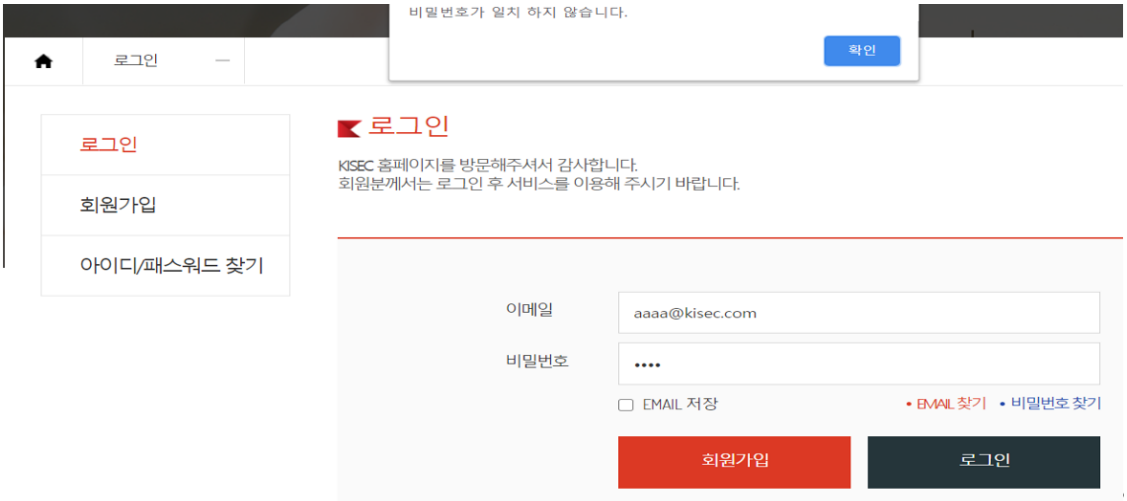
3.9 자동화 공격

취약점 항목	내용
취약점 설명	웹 애플리케이션에 정해진 프로세스에 자동화된 공격을 수행함으로서 자동으로 수많은 프로세스가 진행되는 취약점이다.
점검 결과	로그인 페이지에서 챕차,일회성 확인 로직 구현하지 않았다.
위험요소	로그인에 대한 접근 시도 횟수 제한을 설정하지 않고 자동화 공격을 방치하면, 웹사이트를 다운시키거나 무차별 대입 공격으로 인해 사용자 계정을 탈취할 수 있고, 데이터 등록 또는 메일 발송 기능 등을 이용하여 악의적인 활용이 가능하다.
발생 경로	OO
보안 대책	캡차(이미지를 이용하여 확인 값을 표시하고 사용자가 값을 등록하여 인증함) 등 일회성 확인 로직을 구현해야 한다.

[표 16] 자동화 공격 취약점 개요

❑ 수행 과정

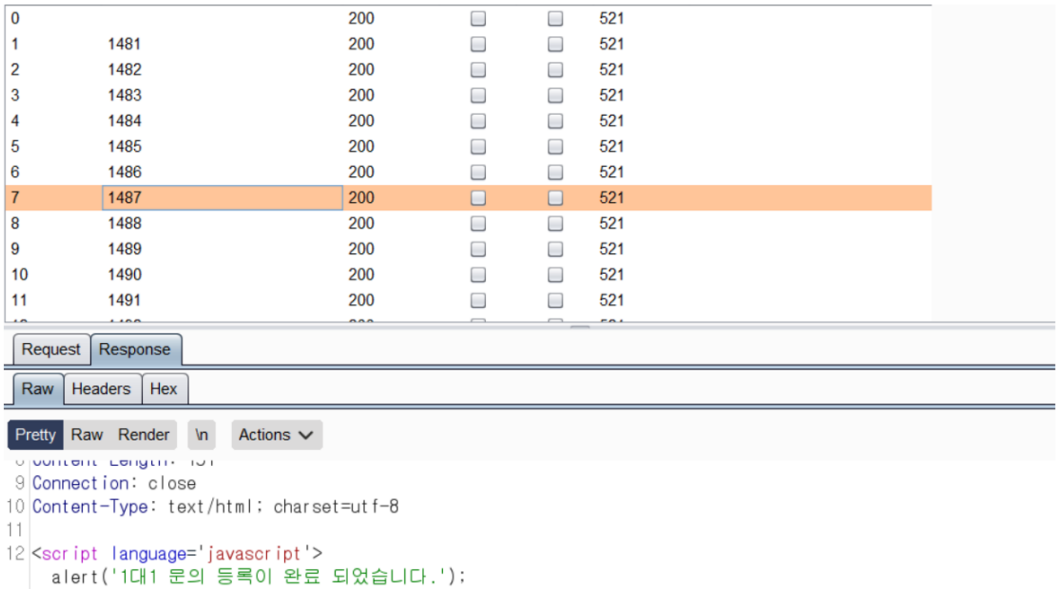
로그인 페이지에서 무차별 공격



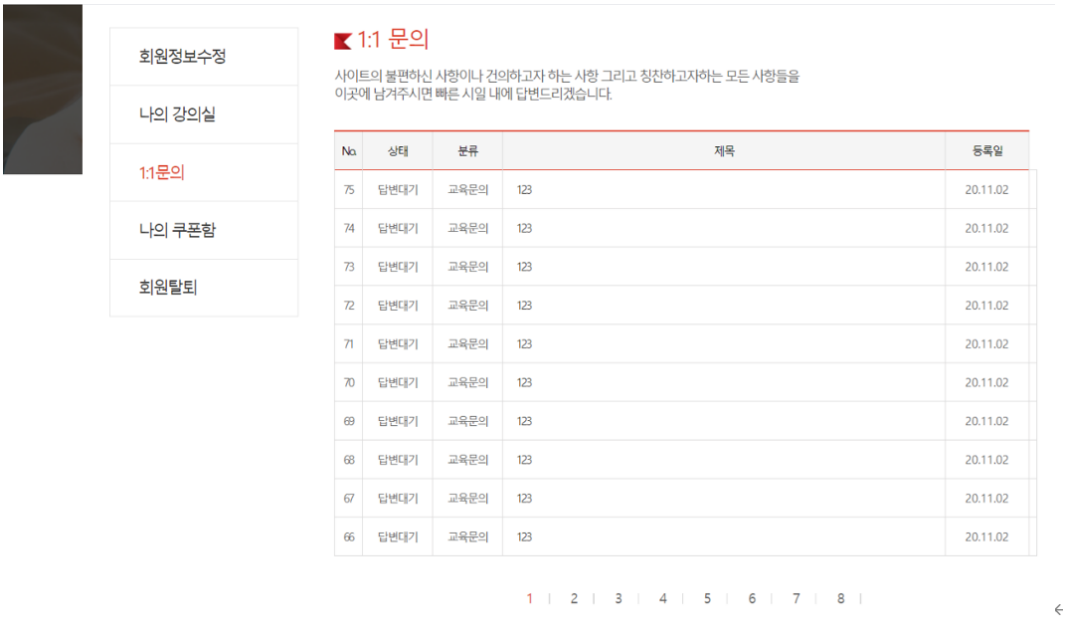
[그림 33] 로그인 페이지에서 로그인 횟수제한없는 화면

❑ 수행 과정

1대1 문의 글 자동화 작성



[그림 34] 1대1 문의 글에 burp sutie 무차별공격 화



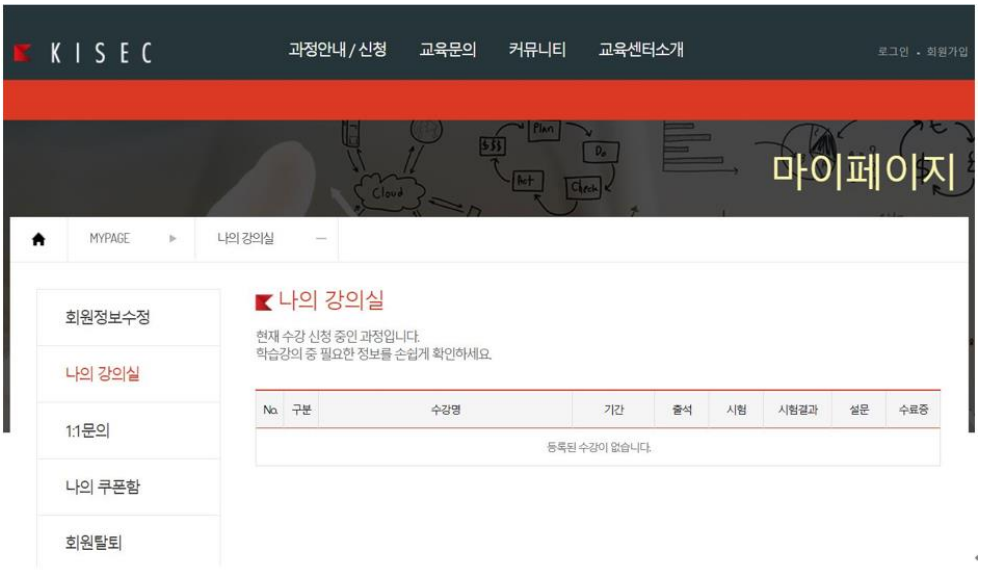
[그림 35] 1대1 문의게시판 무차별공격 결과

3.10 프로세스 검증 누락

취약점 항목	내용
취약점 설명	미흡한 인증처리 과정으로 인해 발생하는 취약점으로, 공격자가 인증을 우회하여 비인가 적인 행위를 할 수 있다.
점검 결과	Mypage 경로를 URL 접근 시 별다른 인증없이 접근이 가능하다.
위험요소	비로그인 상태에서 mypage 접근이 가능하였다.
발생 경로	OO
보안 대책	비 로그인 시 마이페이지로 가는 버튼 비 활성화만 할 것이 아니라 페이지 자체적으로도 비로그인자는 접근이 불가능하게 해야 한다.

[표 17] 프로세스 검증 누락 취약점 개요

❏ 수행 과정



[그림 36] mypage 접근

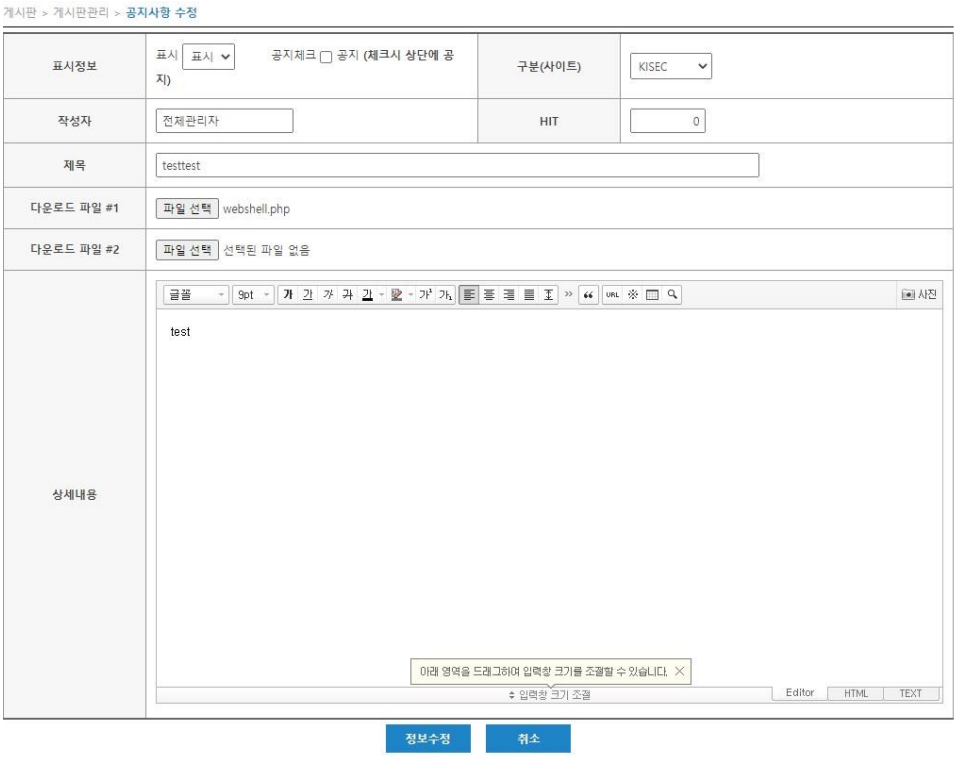
3.11 파일 업로드

취약점 항목	내용
취약점 설명	웹 서버에서 실행 가능한 웹프로그램 파일을 게시판을 통해 검증없이 올릴 수 있다.
점검 결과	Php파일을 아무런 조작도 하지않고 게시판에 올릴 수 있다.
위험요소	서버에 악영향을 미칠 수 있는 코드가 저장될 수 있다.
발생 경로	OO
보안 대책	업로드 가능한 파일을 제한하고 저장되기 전 파일의 내용을 검사해야 한다.

[표 18] 파일 업로드 취약점 개요

❑ 수행 과정

불필요한 php파일도 저장이 가능하다.



[그림 37] 확장자 검사 없이 저장되는 php파일

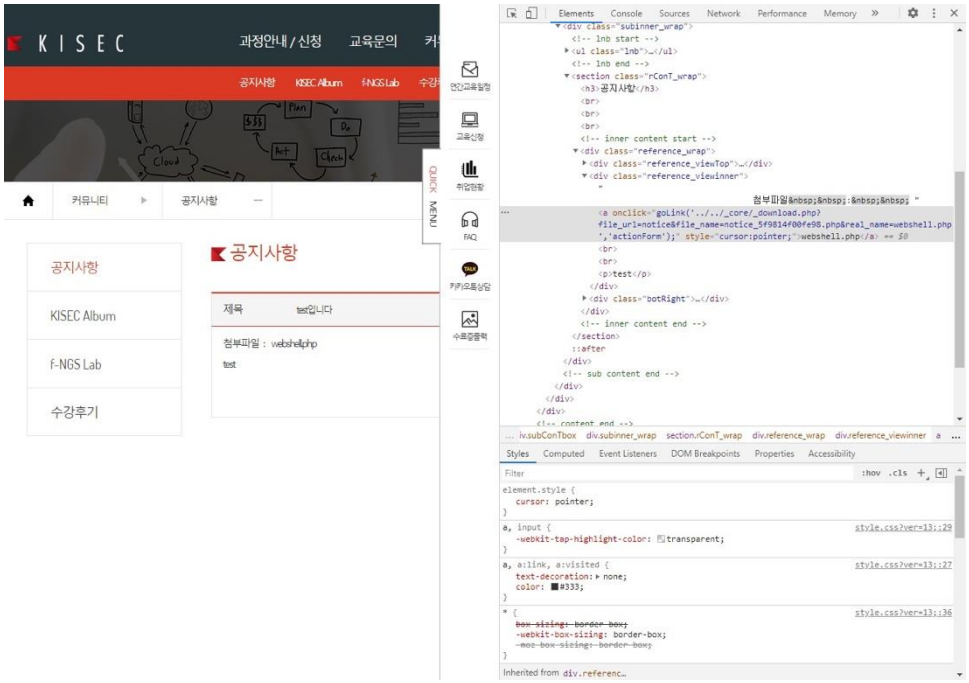
3.12 파일 다운로드

취약점 항목	내용
취약점 설명	상대경로를 조작해서 다른 파일을 다운받을 수 있다.
점검 결과	서버 내부의 권한이 허락되는 파일들을 모두 다운받을 수 있었다.
위험요소	디렉토리 리스팅으로 얻어낸 웹서버의 구조를 이용하여 웹서버 운영에 사용되는 실제 파일들을 다운받을 수 있다.
발생 경로	OO
보안 대책	웹서버 계정의 권한을 제한하여 서버 내 홈페이지 운영과 관련 없는 파일에 대한 접근을 제한해야 한다.

[표 19] 파일 다운로드 취약점 개요

❏ **수행 과정**

파일의 상대 경로를 조작하여 다른 경로의 파일을 다운받을 수 있다.



[그림 38] 상대경로를 조작하여 실제 서버에 존재하는 파일 다운

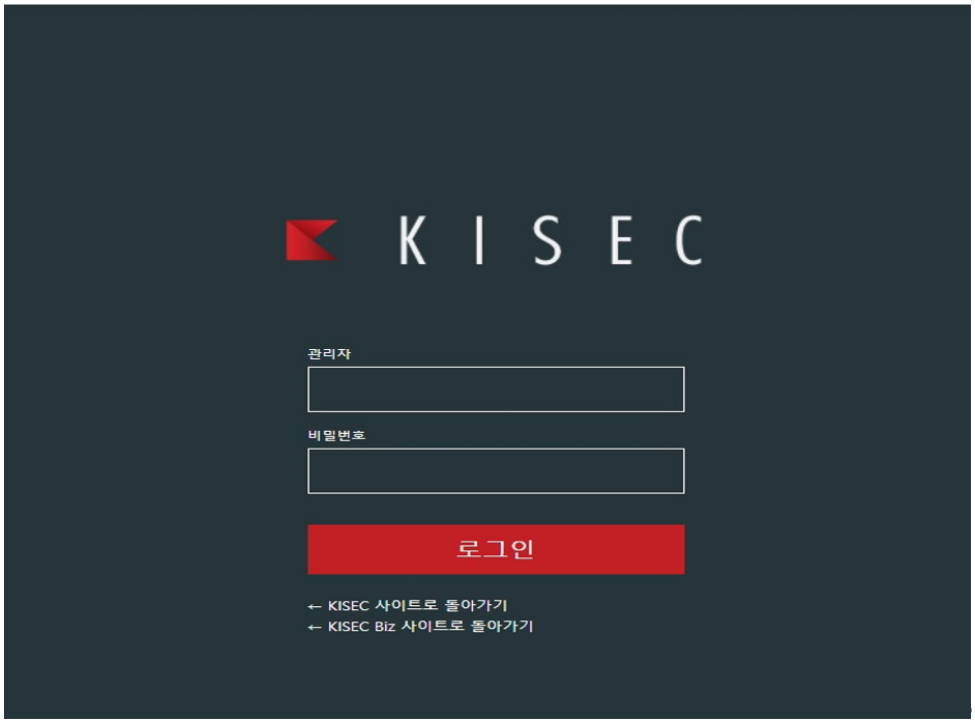
3.13 관리자 페이지 노출

취약점 항목	내용
취약점 설명	인가되지 않은 사용자가 관리자 페이지에 접근할 수 있다.
점검 결과	유추하기 쉬운 admin 이름을 사용하여 관리자 페이지에 접근한다.
위험요소	관리자 계정으로 로그인을 시도할 수 있다.
발생 경로	OO
보안 대책	유추하기 어려운 이름과 포트번호 변경, 지정된 IP만 접속 가능하도록 제한해야 한다.

[표 20] 관리자 페이지 노출 취약점 개요

❏ **수행 과정**

관리자 페이지에 인증없이 접근할 수 있다.



[그림 39] 관리자 페이지 노출

3.14 데이터 평문 전송

취약점 항목	내용
취약점 설명	서버와 클라이언트간 통신 시 암호화하여 전송을 하지 않아 중요 정보 등이 평문으로 전송되는 취약점이다.
점검 결과	회원정보 등 민감한 데이터 전송이 평문으로 노출된다.
위험요소	공격자의 중간자 공격등에 의해 정보가 탈취될 수 있다.
발생 경로	OO
보안 대책	민감한 데이터가 전송되는 구간의 HTTPS 통신 암호화를 적용시켜야 한다.

[표 21] 데이터 평문 전송 취약점 개요

❏ **수행 과정**

중요정보 통신에서 암호화되지않고 평문 전송이 이루어지고 있다.

[그림 40] 로그인 평문 전송

```
----------------------------115620926220389056261172985294
Content-Disposition: form-data; name="mm_cell_1"

010
----------------------------115620926220389056261172985294
Content-Disposition: form-data; name="mm_cell_2"

1234
----------------------------115620926220389056261172985294
Content-Disposition: form-data; name="mm_cell_3"

1234
----------------------------115620926220389056261172985294
Content-Disposition: form-data; name="emailID"

tess
----------------------------115620926220389056261172985294
Content-Disposition: form-data; name="emailDomain"

kisec.com
----------------------------115620926220389056261172985294
Content-Disposition: form-data; name="select"

kisec.com
----------------------------115620926220389056261172985294
Content-Disposition: form-data; name="user_pass"

tess123!
----------------------------115620926220389056261172985294
Content-Disposition: form-data; name="re_pass"

tess123!
----------------------------115620926220389056261172985294
Content-Disposition: form-data; name="mm_company"


----------------------------115620926220389056261172985294
Content-Disposition: form-data; name="mm_grade"
```

[그림 41] 회원가입 평문 전송

```
user_id=bbbb%40kisec.com&user_idx=1407&Mode=secede_member&user_pass=test123!&re_pass=test123!
&withdrawal=%ED%83%88%ED%87%B4%ED%85%8C%EC%8A%A4%ED%8A%B8HTTP/1.1 200 OK
```

[그림 42] 회원탈퇴 평문 전송

```
up_member
----------------------------267201677623251230708934036
Content-Disposition: form-data; name="mm_email"

bbbb@kisec.com
----------------------------267201677623251230708934036
Content-Disposition: form-data; name="old_pass"

3b3e9bf9e01962fe4fb9ef658533392e
----------------------------267201677623251230708934036
Content-Disposition: form-data; name="mm_name"

bbbb
----------------------------267201677623251230708934036
Content-Disposition: form-data; name="mm_phone_1"

0
----------------------------267201677623251230708934036
Content-Disposition: form-data; name="mm_cell_2"

1234
----------------------------267201677623251230708934036
Content-Disposition: form-data; name="mm_cell_3"

1234
----------------------------267201677623251230708934036
Content-Disposition: form-data; name="mm_company"

coupnag
----------------------------267201677623251230708934036
Content-Disposition: form-data; name="mm_grade"

daeri
----------------------------267201677623251230708934036--
```

[그림 43] 회원수정 평문 전송

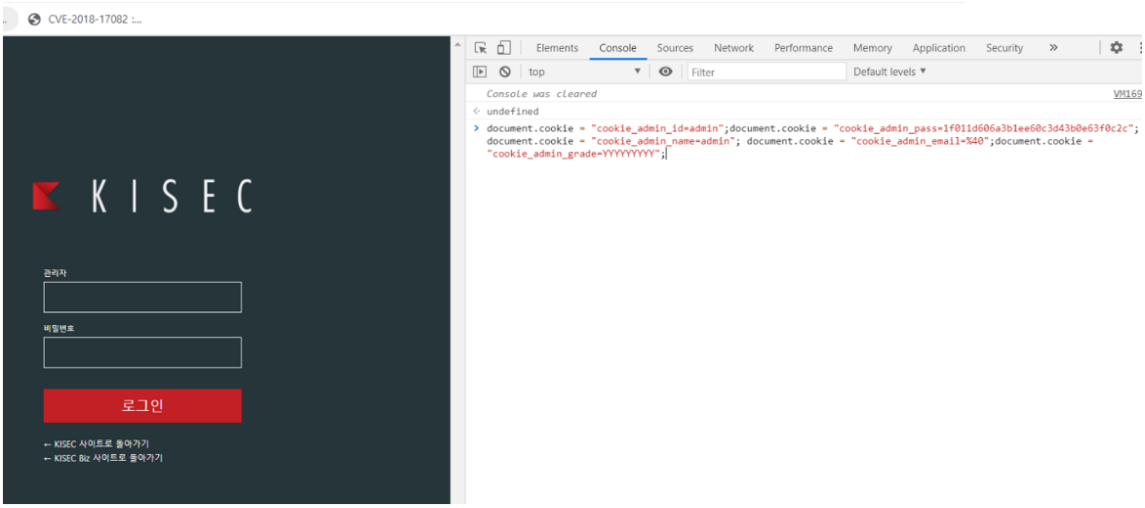
3.15 쿠키값 변조

취약점 항목	내용
취약점 설명	보호되지 않은 쿠키를 사용하여 쿠키 인젝션 등과 같은 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 상승이 가능하다.
점검 결과	쿠키를 사용하고 안전한 알고리즘으로 암호화하지 않고 공격자가 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 변경 가능 하다.
위험요소	쿠키의 조작을 통해 다른 사용자의 유효한 세션을 취득하고 중요 정보 유출 및 변조가 발생할 수 있다.
발생 경로	OO
보안 대책	쿠키 대신 Server Side Session 방식을 사용하거나 쿠키를 통해 인증 등 중요한 기능을 구현해야 할 경우에 안전한 알고리즘 적용해야 한다.

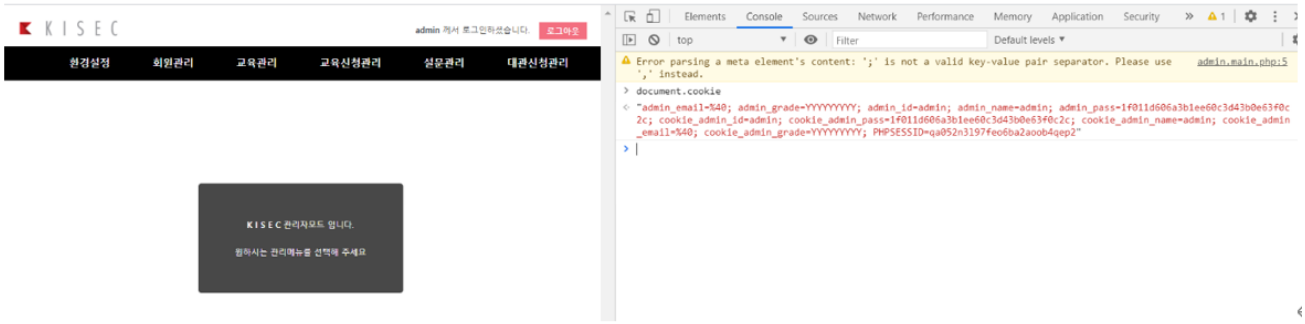
[표 22] 쿠키값 변조 취약점 개요

❑ 수행 과정

어드민페이지 쿠키변조로 로그인가능하다.



[그림 44] 쿠키변조로 로그인



[그림 45] 쿠키변조로 로그인 성공

4. 보호 대책

4.1 SQL 인젝션 취약점

웹 파라미터에 SQL구문을 이용하여 쿼리를 조작할 수 있는 취약점으로, DB내의 개인정보가 유출되어 2차공격의 중요한 정보를 제공할 수 있는 취약점이다.

4.1.1 취약점 대책

권고사항	내용
소스코드 수정 (문자 필터링)	웹 애플리케이션 개발 시 SQL 인젝션 공격을 유발시킬 수 있는 문자들을 필터링 하여 사용하지 못하도록 한다. ※ addslashes등 함수 사용
Database 운영 레벨 수정	DB계정에 최소 권한만을 부여한다. DB계정에 system권한(root)을 부여해서는 안된다.
프로그래밍 예시	function sanitizeString($var) { global $connection; $var = strip_tags($var); $var = htmlentities($var); if(get_magic_quotes_gpc()) $var = stripcslashes($var); return $connection->real_escape_string($var); }

[표 23] SQLi 취약점 대책

4.2 디렉토리 인덱싱 취약점

요청 파일이 존재하지 않을 때 자동적으로 디렉토리 리스트를 출력하는 취약점으로 외부에 노출되지 않은 파일까지 노출이 될 수 있는 취약점이다.

4.2.1 취약점 대책

권고사항	내용
웹 서버 설정 변경	서버 설정파일에서 아래의 붉은 부분을 제거하여 준다. 파일명: apache.conf or httpd.conf 인덱싱 취약점 존재 <Directory /> Options **Indexes** FollowSymLinks AllowOverride All </ Directory>

[표 24] 디렉토리 인덱싱 취약점 대책

4.3 정보 누출

웹 사이트의 민감한 정보가 노출되는 것으로 개발 과정의 코멘트나 에러 메시지 등에서 의도하지 않게 정보가 노출되는 취약점이다.

4.3.1 취약점 대책

권고사항	내용
서버 설정 변경	[php.ini] expose_php = Off [apache.conf or httpd.conf] ServerTokens Prod ServerSignature Off

[표 25] 정보 누출 취약점 대책

4.4 크로스사이트 스크립팅

스크립트를 정상적으로 사용, 동작이 가능한 취약점으로 악성 스크립트가 삽입되거나, 계정정보 탈취가 발생할 수 있는 취약점이다.

4.4.1 취약점 대책

<table>
<tr><th>권고사항</th><th>내용</th></tr>
<tr><td>소스코드 수정
(문자 필터링 or 치환)</td><td>프로그래밍을 할 시 사용자가 문자열에 스크립트를 삽입하여 실행하는 것을 막기 위해 사용자가 입력한 문자열에서 <,> 를 필터링하여 치환한다
<table>
<tr><th>From</th><th>To</th></tr>
<tr><td><</td><td><</td></tr>
<tr><td>></td><td>></td></tr>
</table></td></tr>
<tr><td>프로그래밍 예시</td><td>$text_str = str_replace(“<”, “&lt”, $text_str);
$text_str = str_replace(“>”, “&gt”, $text_str);</td></tr>
</table>

[표 26] XSS 취약점 대책

4.5 불충분한 인증

중요 정보(회원정보 등) 페이지에 대한 인증 절차가 불충분한 경우 발생하는 취약점으로 권한이 없는 사용자가 중요 정보 페이지에 접근하여 정보를 유출하거나 변조 가능한 취약점이다.

4.5.1 취약점 대책

권고사항	내용
소스코드 수정	[민감한 정보 접근 2차인증] 민감한 정보 수정이 이루어지는 페이지의 사용자 패스워드 재확인과 같은 2차적으로 인증 가능한 프로세스를 추가한다. [패스워드 규칙 서버측 확인] 클라이언트에서만 패스워드 규칙을 확인하는 것이 아니라 전송된 값을 서버에서도 규칙 부합 여부를 판단하는 프로세스를 추가한다.

[표 27] 불충분한 인증 취약점 대책

4.6 불충분한 인가

중요 정보 페이지 접근을 위한 인증 로직이 구현되지 않을 경우, 비인가 사용자의 페이지에 접근 및 중요 정보의 열람 빛 변조가 가능한 취약점이다.

4.6.1 취약점 대책

권고사항	내용
소스코드 수정 (세션인증)	프로그래밍을 할 때 세션인증이 필요한 페이지에는 세션인증을 하는 코드를 삽입하고, 세션이 존재하지 않다면 접근이 불가능하게 설정해야 한다.
프로그래밍 예시	하나의 프로세스는 일반적으로 여러 개의 페이지로 이루어지므로 접근 통제를 구현하고 있는 코드는 구조화 모듈화가 되어 있어야 권한 체크가 누락되는 것을 방지할 수 있다. 또한, 인증 과정을 처리하는 부분에 Client Side Script(Javascript, VBScript 등)를 사용하면 사용자가 임의로 수정할 수 있으므로 Server Side Script(ASP, PHP, JSP)를 통하여 인증 및 필터링 과정이 수행되어 야 한다. 히든 필드에 저장된 값은 소스보기로 확인할 수 있으므로 중요정보는 서버 측 세션을 사용 하여 페이지 상에서 노출되지 않도록 구현한다. 불가피하게 사용 시 반드시 암호화하여 사용하고 서버 측에서 무결성을 검증해야 한다.

[표 28] 불충분한 인가 취약점 대책

4.7 불충분한 세션 만료

세션 타임아웃을 너무 길게 설정하거나 세션만료가 되지 않아 세션을 재사용 할 수 있는 취약점이다.

4.7.1 취약점 대책

권고사항	내용
세션 타임아웃 설정	세션 ID는 로그인 시 마다 새로운 세션 ID를 발급받도록 하며, 세션 타임아웃 설정을 통해 일정 시간(10분) 동안 움직임이 없을 경우 자동 로그아웃 되도록 한다.
프로그래밍 예시	$_SESSION['entry_time'] = time(); if((time() - $_SESSION['entry_time']) > 600) { header('login.php'); exit; }

[표 29] 불충분한 세션 만료 취약점 대책

4.8 세션 고정

세션 하이재킹 기법의 하나로 유효한 유저 세션을 탈취하여 인증을 우회하는 취약점이다

4.8.1 취약점 대책

권고사항	내용
새로운 세션ID 발급	로그인과 같은 인증절차가 진행된 후 인증된 세션은 신규 세션 발행을 하여 탈취된 세션이 주입하여도 우회 할 수 없도록 조치하여야 한다. 만약 신규 세션을 발행할 수 없는 경우에는 인가시점에 쿠키상에 별도의 토큰을 발행하여 매 요청별로 세션영역에 보관된 토큰과 매칭을 시키는 방법 또한 하나의 방법이다.

[표 30] 세션 고정 취약점 대책

4.9 자동화 공격

웹 어플리케이션의 특정 프로세스를 반복 수행함으로서 자동으로 수많은 프로세스(대량 스팸 메일 발송 등) 가 진행되는 취약점이다.

4.9.1 취약점 대책

권고사항	내용
접근시도 횟수 설정	특정 시간 내 동일 프로세스가 반복 실행되지 않도록 시간제한 및 CAPTCHA 인증을 적용하고, 또한, 자동화공격에 의한 시스템 과부하를 방지하기 위한 점검은 보안 솔루션을 통해 대량의 패킷이 유입되는지 모니터링 해야 한다.

[표 31] 자동화 공격 취약점 대책

4.10 프로세스 검증 누락

미흡한 인증처리 과정으로 인해 발생 하는 취약점으로, 공격자가 인증을 우회하여 비인가 적인 행위를 할 수 있다.

4.10.1 취약점 대책

권고사항	내용
소스코드 수정 (로그인 권한 확인)	로그인 권한이 필요한 페이지를 이용할 시 로그인 여부를 확인할 수 있는 세션 값을 설정하여 로그인이 정상적인지 점검하는 코드를 추가, 인증하여야 한다.

[표 32] 프로세스 검증 누락 취약점 대책

4.11 파일 업로드

웹 서버에 악성 스크립트 파일(asp, php, jsp)을 업로드 후 웹을 통해 해당 시스템을 제어할 수 있는 취약점이다.

4.11.1 취약점 대책

권고사항	내용
소스코드 수정 (업로드 확장자 확인)	업로드가 허용된 확장자만 가능토록 Server Side에서 컨트롤 해줘야하고 허용할 확장자를 제외한 모든 파일의 업로드를 금지하는 White list 방식의 필터링을 적용해야한다. 또한 확장자 검사를 할 때, 대소문자 구분 없이 비교해야하며.jpg.php 와 같은 이중확장자나 끝에 "."을 추가하는 trick에 주의하며 처리해야한다.
프로그래밍 예시	<? //확장자 검사 //$filename: 파일명 //$avaext: 허용할 확장자 예) $avaext = "jpg,gif,pdf" //리턴값: true-"ok", false-"error" function checkext($filename,$avaext) { if(eregi("₩0", $filename)) { return "error"; } //업로드 금지 확장자 체크 if(eregi('₩.inc\|₩.htm\|₩.shtm\|₩.ztx\|₩.dot\|₩.cgi\|₩.pl\|₩.phtm\|₩.php\|₩.ph',$filename)) return "error"; //허용 확장자가 설정된 경우 if ($avaext != "") { $extfile = str_replace(",","|₩₩.", $avaext); $extfile = "₩₩." . $extfile; if(eregi($extfile,$filename)) return "ok"; } return "error"; } ?>

[표 33] 파일 업로드 취약점 대책

4.12 파일 다운로드

파일다운로드 기능을 제공하는 스크립트 파일의 파라미터를 조작하여 임의의 파일을 다운 받을 수 있는 취약점이다.

4.12.1 취약점 대책

권고사항	내용
소스코드 수정 (경로 문자 필터링)	다운로드 모듈의 경로를 처리하는 파라미터 변수에 대해서 [../], [..₩], [./]를 필터링해야 한다.
프로그래밍 예시	<? //다운로드 경로 체크 함수 //$dn_dir - 다운로드 디렉토리 경로(path) //$fname - 다운로드 파일명 //리턴 - true: 다운로드 파일 경로, false: "error" function checkpath($dn_dir,$fname) { //구분자 통일 $dn_dir = str_replace("₩₩","/", $dn_dir); //다운로드 경로에 공격 문자 필터링 if (eregi("₩.₩./",$dn_dir)) { print "허용하지 않는 입력 값입니다."; return "error"; } //사용자 입력값으로 다운로드 파일 경로 생성 $dn_file = $dn_dir . "/" . $fname; //$fname에서 파일명만 분리 - 파일명에 공격 위험성 문자 필터링 $filename=basename($fname); $strfname = $dn_dir . "/" . $filename; //사용자 입력값과 재구성한 입력값을 비교하여 공격 위험성이 존재하는지 확인 if ($strfname == $dn_file) return $strfname; else return "error"; } ?>

[표 34] 파일 다운로드 취약점 대책

4.13 관리자 페이지 노출

홈페이지 관리 기능이 제공되는 관리자 페이지 주소가 노출, 또는 추측가능하여 외부에서 접속할 수 있는 취약점이다.

4.13.1 취약점 대책

권고사항	내용
관리자 페이지 분리 및 적절한 접근 통제	관리자 페이지는 아래와 같은 보안정책에 의해 보호되어야 한다. ● 관리자 페이지는 일반 사용자용 인터페이스와 분리되어 작성되어야 한다. (별도의 포트, 도메인 등) ● 관리자 페이지는 임의의 위치에서 접근할 수 없도록 적절한 접근 통제 절차가 적용되어야 한다. (IP 접근 제어, SMS 인증 등) ● 추측하기 쉬운 디렉토리명이나 파일명을 사용해서는 안된다.

[표 35] 관리자 페이지 노출 취약점 대책

4.14 데이터 평문 전송

서버와 클라이언트간 통신 시 중요정보가 평문으로 노출되는 취약점이다.

암호화는 신용카드나 건강정보, 개인정보들과 같은 민감한 데이터를 전송할 때에는 반드시 사용해야한다.

4.14.1 취약점 대책

권고사항	내용
데이터 암호화	개인정보(아이디, 비밀번호, 주민등록 번호, 전화번호, 계좌번호, 계좌 비밀번호, 게시판 등에서 사용되는 성명, 이메일, 연락처 등) 를 다루는 사이트는 SSL 인증서, 또는 암호화 응용프로그램을 설치하여 개인정보 암호화 송・수신을 해야 한다

[표 36] 데이터 평문 전송 취약점 대책

4.15 쿠키 변조

사용자 인증 방식 중 하나인 쿠키를 변조하여 다른 사용자 도용, 권한 상승, 인증우회가 가능한 취약점이다.

4.15.1 취약점 대책

권고사항	내용
Cookie 대신 Session을 사용	Cookie를 사용할 경우 SEED, 3DES, AES 등 공인된 암호화 알고리즘을 사용하여 암호화를 적용하고, 가급적이면 Cookie 대신 Session 방식을 사용한다. Session 방식은 접속자 별로 세션을 생성하여 사용자의 정보를 각각 저장할 수 있는 오브젝트로써 페이지의 접근을 허가하거나 금지할 때 또는 사용자 별로 정보를 저장할 때 많이 사용된다. 클라이언트의 자원을 사용하는 쿠키와는 달리 세션은 서버 쪽의 자원을 사용하고 있어 보안성이 높다고 할 수 있으므로, 세션방식을 채택하는 것이 바람직하다.

[표 37] 쿠키 변조 취약점 대책